Claims

We claim:

1. A method of generating IP identification numbers for IP datagrams, comprising the steps of:

maintaining a plurality of IP identification number generators;

associating a plurality of receiving stations with the plurality of IP identification number generators such that each receiving station has an IP identification number generator associated therewith; and

generating an IP identification number for a datagram sent to one of the receiving stations based on an output of the associated IP identification number generator.

2. A method as in claim 1, wherein each of the IP identification number generators has at least one receiving station associated therewith.

3. A method as in claim 1, wherein at least one of the IP identification number generators has plural receiving stations associated therewith.

4. A method as in claim 1, wherein the plurality of IP identification number generators forms an array of number generators.

5. A method as in claim 4, wherein the array of number generators is an array of counters.

6. A method as in claim 5, wherein the counters are 16-bit counters.

7. A method as in claim 4, wherein the plurality of IP identification number generators is associated with the plurality of receiving stations by hashing destination addresses for the receiving stations so as to form an index to the array.

8. A method as in claim 4, wherein the plurality of IP identification number generators is associated with the plurality of receiving stations by hashing destination addresses for the receiving stations and protocols for transmitting to those receiving stations so as to form an index to the array.

9. A method as in claim 8, wherein hashing is performed such that at least half of the number generators in the array are associated with UDP protocol communications.

10. A method as in claim 1, wherein the steps are performed by an IP layer of a sending station's communication system.

Sub A1

11. A method of reducing a likelihood of misassembly of data fragments from fragmented IP datagrams, comprising the steps of:

receiving data fragments of a datagram having an IP identification number; and

discarding all received data fragments of the datagram upon detection of receipt of an overlapping data fragment having the IP identification number, wherein the overlapping data fragment overlaps data in an already-received data fragment.

12. A method as in claim 11, wherein the overlapping data fragment overlaps all of the already-received data fragment.

13. A method as in claim 11, wherein the overlapping data fragment overlaps less than all of the already-received data fragment.

14. A method as in claim 11, wherein the steps are performed by an IP layer of a receiving station's communication system.

15. A method of reducing a likelihood of misassembly of data fragments from fragmented IP datagrams, comprising the step of reducing a timeout for reassembling the datagrams to less than a standard timeout.

16. A method as in claim 15, wherein the data fragment reassembly timeout is reduced to 45 seconds from the standard timeout of 64 seconds.

17. A method as in claim 15, wherein the data fragment assembly timeout is dynamically reduced based on NFS data for round-trip times between a sending station and a receiving station.

18. A method as in claim 15, wherein the step is performed by an IP layer of a receiving station's communication system.

19. A method of reducing a likelihood of misassembly of data fragments from fragmented IP datagrams, comprising the steps of:

receiving data fragments of a datagram having an IP identification number; and

reducing a remaining time for reassembling the datagram upon detection of a gap in the received data fragments.

20. A method as in claim 19, wherein the remaining time for reassembling the datagram is reduced to eight seconds.

21. A method as in claim 19, wherein the steps are performed by an IP layer of a receiving station's communication system.

22. A method of reducing a likelihood of misassembly of data fragments from fragmented IP datagrams, comprising the steps of:

receiving data fragments of a first datagram having a protocol identification number, a source address, and a first IP identification number; and

reducing a remaining time for reassembling the first datagram upon detection, before receipt of a last data fragment of the first datagram, of a data fragment of a second datagram having the protocol identification number and the source address but having a second IP identification number.

23. A method as in claim 22, wherein the remaining time for reassembling the datagram is reduced to eight seconds.

24. A method as in claim 22, wherein the steps are performed by an IP layer of a receiving station's communication system.

25. A method of detecting a likelihood of misassembly of data fragments from fragmented IP datagrams, comprising the steps of:

detecting for communication errors between a sending station and a receiving station; and

determining that the likelihood of misassembly is high upon detection that the communication errors occur at a high rate for a predefined period of time.

26. A method as in claim 25, wherein the communication errors that are detected include communication errors detected by an IP layer of the receiving station's communication system.

27. A method as in claim 26, wherein the communication errors include receipt of overlapping data fragments.

28. A method as in claim 26, wherein the communication errors include IP datagram reassembly timeout errors.

29. A method as in claim 25, wherein the communication errors that are detected include communication errors detected by a UDP layer of the receiving station's communication system.

30. A method as in claim 29, wherein the communication errors include UDP length errors.

31. A method as in claim 29, wherein the communication errors include UDP checksum errors.

32. A method as in claim 25, wherein the communication errors that are detected include communication errors detected by an NFS layer of the sending station's communication system.

33. A method as in claim 25, further comprising the step of implementing policies to reduce the likelihood of misassembly of data fragments upon determining that the likelihood of misassembly is high.

34. A method as in claim 33, wherein implementing the policies further comprises preferentially using TCP instead of UDP.

35. A method as in claim 33, wherein implementing the policies further comprises using additional checksums.

36. A method as in claim 33, wherein implementing the policies further comprises presenting a warning message to a system administrator.

37. A method for a sending station to detect a likelihood of misassembly at a receiving station of data fragments from fragmented IP datagrams, comprising the steps of:

determining a rate at which an IP identification number generator associated with the receiving station wraps around; and

determining that the likelihood of misassembly at the receiving station is high upon determination that the IP identification number generator wraps around at faster than a predetermined rate.

38. A method as in claim 37, wherein the predetermined rate is once every ninety seconds.

39. A method as in claim 37, further comprising the step of implementing policies to reduce the likelihood of misassembly of data fragments upon determining that the likelihood of misassembly is high.

40. A method as in claim 39, wherein implementing the policies further comprises preferentially using TCP instead of UDP.

41. A method as in claim 39, wherein implementing the policies further comprises use of additional checksums.

42. A method as in claim 39, wherein implementing the policies further comprises presenting a warning message to a system administrator.

43. A method as in claim 39, wherein the sending station maintains plural IP identification number generators, and wherein implementing the policies further comprises reducing a number of receiving stations associated with the IP identification number generator that is wrapping around at faster than the predetermined rate.

44. A method for a sending station to detect a likelihood of misassembly at a receiving station of data fragments from fragmented IP datagrams, comprising the steps of:

determining a rate at which an IP identification number generator associated with the receiving station wraps around; and

determining that the likelihood of misassembly at the receiving station is high upon determination both that (a) the IP identification number generator wraps around at faster than a predetermined rate and (b) NFS re-transmissions are higher than a predetermined threshold.

//

//

//

//

//

//

//

//